DoD Critical Infrastructure Protection

NDIA Information Briefing

July 3, 2002

DoD CIP – Executive Summary

Critical Infrastructure Protection

What is CIP?

- **CIP is mission assurance: the identification, assessment, and assurance of cyber and physical assets essential to the mobilization, deployment, and sustainment of U.S. military operations; interdependencies are the key**

Why is it important?

- **Failure of critical assets degrade / disrupt operations; CIP identifies vulnerabilities and risks to missions; CIP will provide real-time, situational awareness of potential / unfolding mission disruption**

Who will benefit?

- **Military commanders, policy makers, DoD counterintelligence & security forces**

What will it cost?

- **~$XX M / year for ~5 years for analysis and assessment (manpower, tools, resulting data)**
- **~$XX M R&D for real-time situational awareness**
- **~$XX M / year for ops support integrated into existing command centers**

When will it be done?

- **First wave within ~5 years**
- **Continues indefinitely when integrated into planning processes**

U.S. Critical Infrastructure Protection

U.S. Intent -- Pursue all necessary measures to eliminate significant vulnerabilities to both physical and cyber attack on critical infrastructures . . .

U.S. Federal Infrastructures		U.S. DoD Infrastructures	
• Telecommunications	⟷	• Global Information Grid	• Command, Control & Communications
• Energy	⟷	• Public Works	• Intelligence, Surveillance & Reconnaissance
• Water systems	⟷	• Public Works	• Personnel
• Transportation	⟷	• Transportation	• Space
• Banking and Finance	⟷	• Financial Services	• Logistics
• Emergency Services	⟷	• Emergency Services	• Health
			• Defense Industrial Base

DoD Scope:
- Domestic and Foreign
- Public and Private Sectors

Requirements for CIP

Presidential Decision Directive 63

Defense Planning Guidance

Executive Order – Critical Infrastructure Protection in the Information Age

Joint Vision 2020

Executive Order – Homeland Security

Contingency Planning Guidance

DoD CIP Plan

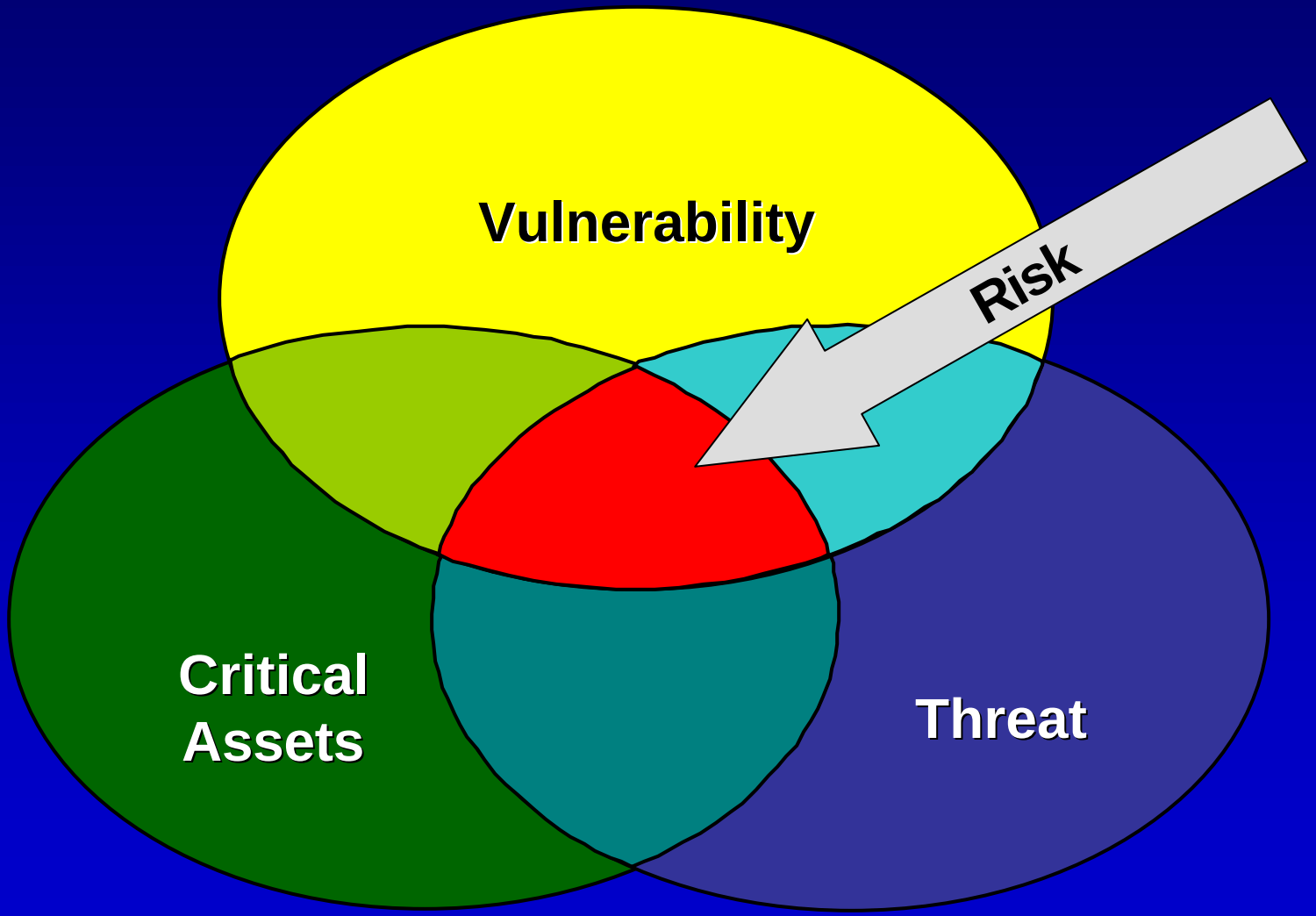
DoD Directive – Critical Infrastructure Protection

DoD CIP Vision

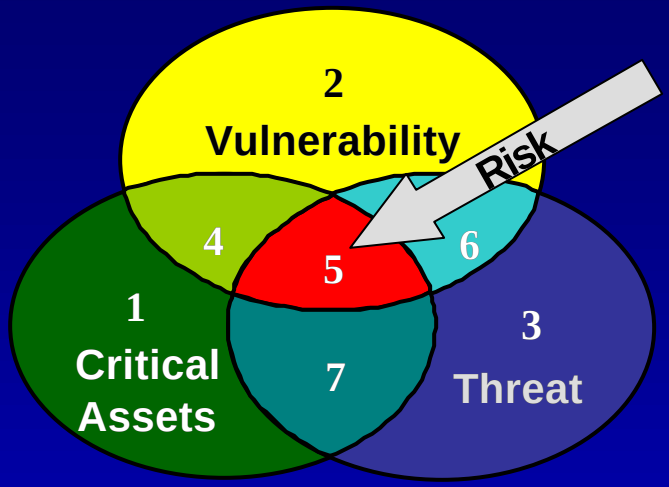
- Critical infrastructure assets DoD depends upon are available to mobilize, deploy and sustain military operations, always
  - Operators have real-time situational awareness of critical infrastructure assets
  - Modeling and simulation reliably depicts / predicts operational environment in sufficient time to change near future events

- Result
  - Infrastructures are fundamentally more reliable and available
  - The enemy is denied advantages
  - Reduced number of single points of failure
  - Can adjust operations in anticipation of infrastructure events

Simple Risk Model



Simple Risk Model



1 – Critical assets (information, systems, programs, people, equipment or facilities) for which there is no known vulnerability and no known threat exposure

2 – Vulnerabilities in systems, programs, people, equipment or facilities that are not associated with critical assets and for which there is no known threat exposure

3 – Threat environment for which there is no known threat to critical assets or access to vulnerabilities (or vulnerability information)

4 – Critical assets for which there are known vulnerabilities, but no known threat exposure

5 – Critical assets for which there are known vulnerabilities and threat exposure

6 – Threat has acquired specific knowledge and/or capability to exploit a vulnerability although not a critical asset vulnerability

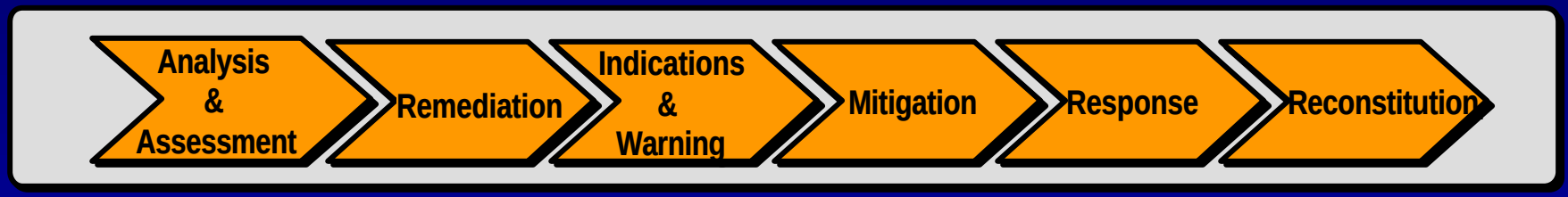
7 – Critical asset for which there are no known vulnerabilities, but there is exposure to a specific threat

#1 – Determine what is most important; identify the critical infrastructure assets
#2 – Prioritize asset assessments based on the threat
#3 – Pick from the critical assets priority list to establish the vulnerability assessment work program
#4 – Evaluate risks from a mission perspective

- Criticality is determined by asset's importance to the mission
- Threat does not determine criticality
- Vulnerability does not determine criticality

DoD CIP Program

Major Program Activities



Analysis & Assessment – What is critical, what are the vulnerabilities, what are the risks and what is the plan remediation?

Remediation – What are the deliberate precautionary measures to improve the reliability, availability, and survivability of critical assets and support systems?

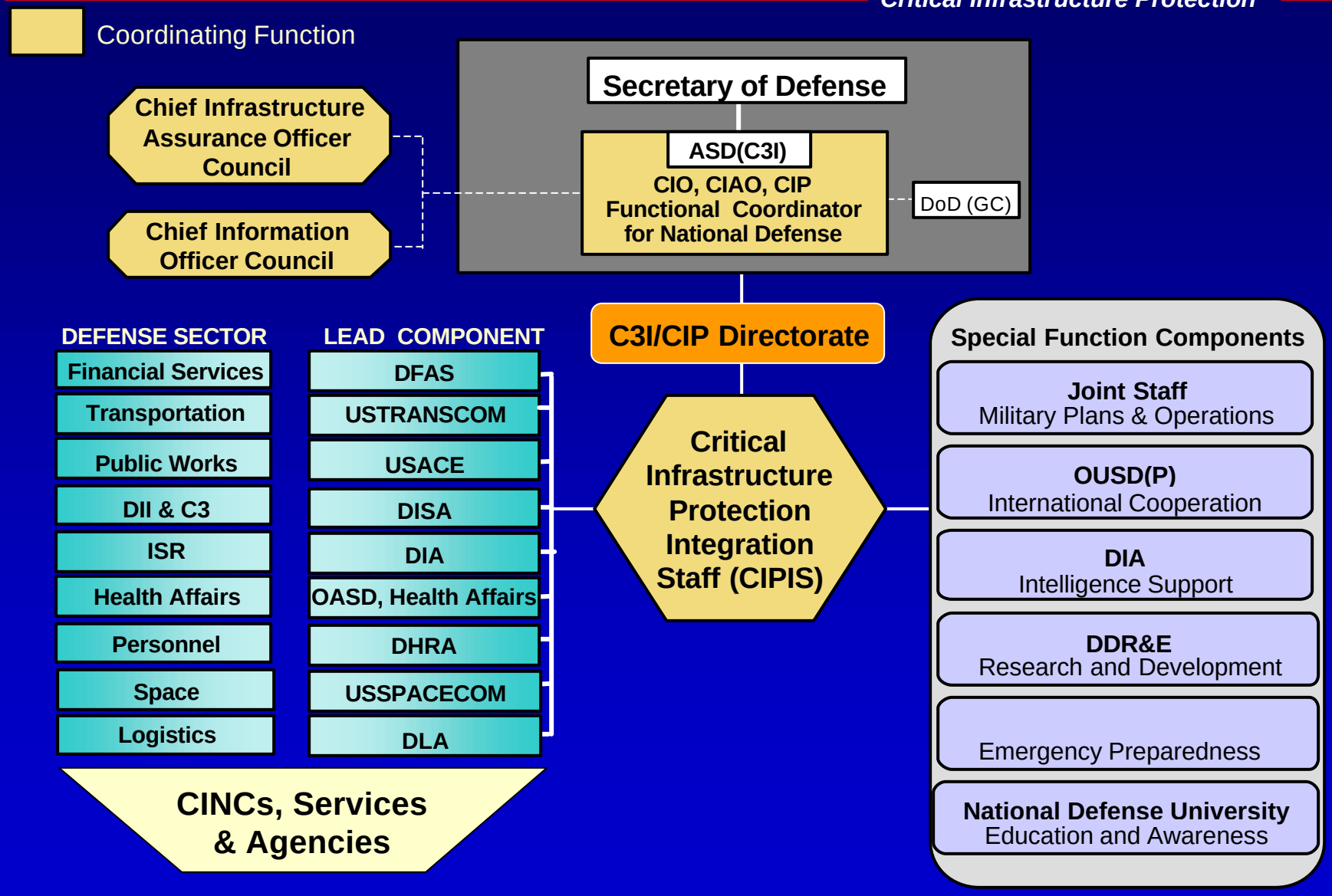
Indications & Warning – What accurate and convincing information must go to decision-makers in sufficient time for them to take action?

Mitigation – What pre-planned and coordinated reactions are needed to reduce or minimize the adverse impact of possible incidents?

Response – What offensive and defensive measures will be implemented to deal effectively with an actual adverse incident?

Reconstitution – Restore critical assets and their necessary infrastructure support systems to pre-incident operational status

DoD CIP Coordination



Challenges

- Coherent, Validated Methodology
  - Identification of Critical Assets
  - Vulnerability Assessment Protocol
  - Risk Assessment Protocol
- Clarity of Threat, Indications and Warning
- Information Sharing Legislation
- Information Protection Guidance
- Outreach and Education

DoD Critical Infrastructure Protection

NDIA Information Briefing

July 3, 2002